CLAIMS

What I claim is:

1. In a system for sending messages over a network between first and second computing units, method comprising the following steps:

(a). computing r components of encrypting key e.sub.1, e.sub.2,..., e.sub.r and r components of decrypting key d.sub.1, d.sub.2,..., d.sub.r according to the following relations:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+... +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and (d.sub.1)+ (d.sub.2)+ ...+(d.sub.r) = (k.sub.2).(p-1).(q-1), where:

p and q are two prime numbers;

k.sub.1 and k.sub.2 are suitable integers; and

encrypting a message M into r cipher versions M.sub.1, M.sub.2, ..., M.sub.r using the r blinded components of the encrypting key e.sub.1 + t, e.sub.2 + t,....,e.sub.r + t as follows:

M.sub.1 = (M.sup.(e.sub.1 + t)) mod n
M.sub.2 = (M.sup.(e.sub.2 + t)) mod n

. . . . . .

. . . . . .

. . . . . .

M.sub.r = (M.sup.(e.sub.r + t)) mod n, where:

n = p.q;

t is a random number generated on encrypting unit and discarded after encryption is complete;

mod represents the remainder left when left hand operand is divided by right hand operand;

or

computing the key components e.sub.1, e.sub.2,..., e.sub.r and d.sub.1, d.sub.2,..., d.sub.r according to the following relation and conditions:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+... +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and each of the values (e.sub.1), (e.sub.2),..., (e.sub.r) has a common factor with (p-1).(q-1), but there is no common factor for all (e.sub.1), (e.sub.2),..., (e.sub.r), (p-1).(q-1), where:

p and q are prime numbers;
k.sub.1 is a suitable integer; and

encrypting a message M into r cipher versions M.sub.1, M.sub.2, ..., M.sub.r using the r components of the encrypting key, e.sub.1, e.sub.2..., e.sub.r as follows:

M.sub.1 = M.sup.(e.sub.1) mod n
M.sub.2 = M.sup.(e.sub.2) mod n

. . . . .

. . . . .

. . . . .

M.sub.r = M.sup.(e.sub.r) mod n, where:

n = p.q;

p and q are two prime numbers;

(b). delivering all the cipher versions of the message individually to the destination unit in source routing mode, or hop-by-hop routing mode with a small time gap between every two consecutive cipher versions;

(c). collecting all the cipher versions at the destination unit;

(d). computing r number of values N.sub.1, N.sub.2, ..., N.sub.r using r components d.sub.1, d.sub.2,...,d.sub.r of decrypting key, where:

N.sub.1= ((M.sub.1).sup.(d.sub.1)) mod n
N.sub.2= ((M.sub.2).sup.(d.sub.2)) mod n
. . . . . .
. . . . . .
. . . . . .
N.sub.r = ((M.sub.r).sup.(d.sub.r)) mod n, where:

n is the same composite number as used for encryption;

(e). reproducing the original message M as follows:

M = (N.sub.1). (N.sub.2)... (N.sub.r) mod n, where:

n is the same composite number as used for encryption.

2. The methods of claim1, comprising the steps of computing the key components.

3. The methods of claim1, comprising the steps of encrypting the message M into r cipher versions M.sub.1, M.sub.2, …, M.sub.r.

4. The method of claim1, comprising the step of blinding the key components (e.sub.1), (e.sub.2),…, (e.sub.r) by adding a random number t and discarding it after encryption is complete.

5. The method of claim1, comprising the step of enforcing the relation (e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+… +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1.

6. The method of claim1, comprising the step of enforcing the relation (d.sub.1)+ (d.sub.2)+ …+(d.sub.r) = (k.sub.2).(p-1).(q-1).

7. The method of claim1, comprising the step of enforcing the condition on the encrypting key components to have a common factor with (p-1) .(q-1), and not all of them have a common factor.

8. The method of claim1, comprising the step of computing the values N.sub.1, N.sub.2, …, N.sub.r.

9. The method of claim1, comprising the step of recovering the original message M from N.sub.1, N.sub.2, …, N.sub.r.

10. A system of claim 1, wherein at lest one encrypted version of the message is bypassed to a secret host that is not exposed to the public while the remaining are directed to the main host, where the bypassed cipher versions are also collected from the secret host.

11. A system of claim 1, wherein redundant cipher versions of a message are generated and delivered to the destination, where they are identified and discarded before decryption.

12. A system of claim 10, wherein the cipher version received at a secret host is further encrypted in a symmetric key encryption method before sending it to the main host, where it is decrypted by the same symmetric key.

13. A system for sending messages over a communications channel, comprising any of the following two options:

(a). an encoder to transform a message M into two or more cipher versions M.sub.1, M.sub.2, ..., M.sub.r as follows:

M.sub.1 = (M.sup.(e.sub.1 + t)) mod n
M.sub.2 = (M.sup.(e.sub.2 + t)) mod n

. . . . . .

. . . . . .

. . . . . .

M.sub.r = (M.sup.(e.sub.r + t)) mod n, where:

t is a random number generated on encrypting machine;

e.sub.1, e.sub.2,..., e.sub.r are encrypting key components computed according to the relations:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+... +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and

(d.sub.1)+ (d.sub.2)+ ...+(d.sub.r) = (k.sub.2).(p-1).(q-1);

p and q are prime numbers, and n = p.q;

k.sub.1 and k.sub.2 are suitable integers;

(d.sub.1), (d.sub.2),…, (d.sub.r) are components of the other key used by the recipient for decrypting the cipher versions into the original message;

a decoder coupled to receive the cipher versions M.sub.1, M.sub.2, …, M.sub.r from the communications channel and to transform them back to the original message M, where M is a function of M.sub.1, M.sub.2, …, M.sub.r and computed as follows:

N.sub.1= ((M.sub.1).sup.(d.sub.1)) mod n
N.sub.2= ((M.sub.2).sup.(d.sub.2)) mod n

. . . . . .

. . . . . .

. . . . . .

N.sub.r = ((M.sub.r).sup.(d.sub.r)) mod n

M = (N.sub.1). (N.sub.2)…. (N.sub.2) mod n.

(b). an encoder to transform a message M into two or more cipher versions M.sub.1, M.sub.2, …, M.sub.r as follows:

M.sub.1 = M.sup.(e.sub.1) mod n
M.sub.2 = M.sup.(e.sub.2) mod n

. . . . . .

. . . . . .

. . . . . .

M.sub.r = M.sup.(e.sub.r) mod n, where:

e.sub.1, e.sub.2,…, e.sub.r are encrypting key components computed according to the following relation and conditions:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+… +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and each of the values (e.sub.1), (e.sub.2),..., (e.sub.r) has a common factor with (p-1).(q-1), but there is no common factor for all the values (e.sub.1), (e.sub.2),..., (e.sub.r), and (p-1).(q-1), where:

p and q are two prime numbers; n = p.q;

k.sub.1 is a suitable integer; and

(d.sub.1), (d.sub.2),..., (d.sub.r) are decrypting key components used by the recipient for decrypting the cipher versions into the original message;

a decoder coupled to receive the cipher versions M.sub.1, M.sub.2, ..., M.sub.r from the communications channel and to transform them back to the original message M, where M is a function of M.sub.1, M.sub.2, ..., M.sub.r and computed as follows:

N.sub.1= ((M.sub.1).sup.(d.sub.1)) mod n
N.sub.2= ((M.sub.2).sup.(d.sub.2)) mod n

. . . . . .

. . . . . .

. . . . . .

N.sub.r = ((M.sub.r).sup.(d.sub.r)) mod n

M = (N.sub.1) .(N.sub.2) .... (N.sub.r) mod n.

14. A computer-readable medium having computer-executable instructions causing the computer to compute the following:

key components (e.sub.1), (e.sub.2),..., (e.sub.r) and (d.sub.1), (d.sub.2),..., (d.sub.r) according to the relations as follows:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+… +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and

(d.sub.1)+ (d.sub.2)+ …+(d.sub.r) = (k.sub.2).(p-1).(q-1), where:

p and q are prime numbers; and

k.sub.1 and k.sub.2 are suitable integers;

cipher versions of the original message M as follows:

M.sub.1 = (M.sup.(e.sub.1 + t)) mod n
M.sub.2 = (M.sup.(e.sub.2 + t)) mod n

. . . . . .

. . . . . .

. . . . . .

M.sub.r = (M.sup.(e.sub.r + t)) mod n, where:
t is a random number generated on encrypting machine and discarded after encryption is complete.

original message as follows:

N.sub.1= ((M.sub.1).sup.(d.sub.1)) mod n
N.sub.2= ((M.sub.2).sup.(d.sub.2)) mod n

. . . . . .

. . . . . .

. . . . . .

N.sub.r = ((M.sub.r).sup.(d.sub.r)) mod n

M = (N.sub.1). (N.sub.2)… (N.sub.r) mod n

15. A computer-readable medium of claim 14, having computer-executable instructions that differ in computing key components and encrypting a message as follows:

computing key components (e.sub.1), (e.sub.2),..., (e.sub.r) and (d.sub.1), (d.sub.2),..., (d.sub.r) according to the relations as follows:

(e.sub.1). (d.sub.1)+ (e.sub.2). (d.sub.2)+... +(e.sub.r). (d.sub.r) = (k.sub.1).(p-1).(q-1) + 1

and each of the values (e.sub.1), (e.sub.2),..., (e.sub.r) has a common factor with (p-1).(q-1), but there is no common factor for all the values (e.sub.1), (e.sub.2),..., (e.sub.r), and (p-1).(q-1), where:

p and q are two prime numbers; n = p.q;
k.sub.1 is a suitable integer; and

encrypting original message into r cipher versions as follows:

M.sub.1 = M.sup.(e.sub.1) mod n
M.sub.2 = M.sup.(e.sub.2) mod n

. . . . .

. . . . .

. . . . .

M.sub.r = M.sup.(e.sub.r) mod n, where:
t is a random number generated on encrypting machine and discarded after encryption is complete.